ACTION MEMO

September 11, 2006; 3 p.m.

FOR: ASSISTANT SECRETARY OF DEFENSE (HEALTH AFFAIRS)

FROM: Carl E. Hendricks, Chief Information Officer (Military Health System)
(//s//06/30/06)

SUBJECT: Military Health System Information Assurance Implementation Guide Number 15 for Identity Protection

- This memo promulgates the Information Assurance Implementation Guide Number 15 for Identity Protection (IdP). It provides guidance for accomplishing Department of Defense (DoD) electronic IdP activities within the Military Health System (MHS) and supplements the direction provided in DoD Directive (DoDD) 1000.25, "Personnel Identity Protection (PIP) Program." The guide is for use in conjunction with "Military Health System Information Assurance Policy Guidance," March 5, 2004.

- The guide is subject to bi-annual review and revision.

- The guide was approved by the MHS Information Assurance Working Group on December 9, 2005 and the Enterprise Architecture Board members concurred on April 26, 2006.

RECOMMENDATION: That the ASD (HA) sign the memo at TAB A.

COORDINATION: TAB B

Attachments:
As stated

Prepared by: Clarissa Reberkenny, Director, Technology Management, Integration and Standards, (703) 681-8786, DOCS Open # 107143, 109629

MEMORANDUM FOR DEPUTY DIRECTOR, TRICARE MANAGEMENT
ACTIVITY
DEPUTY SURGEON GENERAL OF THE ARMY
DEPUTY SURGEON GENERAL OF THE NAVY
DEPUTY SURGEON GENERAL OF THE AIR FORCE
PROGRAM EXECUTIVE OFFICER, JOINT MEDICAL
INFORMATION SYSTEMS OFFICE

SUBJECT: Military Health System Information Assurance Implementation
Guide Number 15 for Identity Protection

This memorandum authorizes the distribution of the attached Information Assurance Implementation Guide Number 15 for Identity Protection (IdP), and is to be used in conjunction with "Military Health System (MHS) Information Assurance Policy Guidance," March 5, 2004. This implementation guide was developed in collaboration with the MHS Information Assurance Working Group (IAWG), and reviewed and approved by IAWG membership. It was coordinated and approved by the MHS Technical Integration Working Group, the Service Medical Chief Information Officers, and the MHS Enterprise Architecture Board. It provides guidance for accomplishing Department of Defense (DoD) electronic IdP activities within the MHS, and supplements the direction provided in DoD Directive (DoDD) 1000.25, "Personnel Identity Protection (PIP) Program." It will be reviewed bi-annually and updated as needed.

This guidance applies to the TRICARE Management Activity, Joint Medical Information Systems Office, and TRICARE contractors if required by contract. The guide shall be promulgated throughout the MHS. The Chief Information Officers of the Service Medical Departments are encouraged to incorporate this document into their information assurance policies and procedures.

For additional information, please contact Mr. Daniel Brooks, Director, MHS Identity Protection and Management/Public Key Infrastructure Program, at (703) 681-6867, or *Daniel.Brooks@tma.osd.mil*.

William Winkenwerder, Jr., MD

Attachment:
As stated

<table>
<tr><td rowspan="2"><b>MILITARY HEALTH SYSTEM (MHS)</b>

<b>INFORMATION ASSURANCE (IA)
IMPLEMENTATION GUIDE</b></td><td colspan="2"><b>IMPLEMENTATION GUIDE No. 15</b></td></tr>
<tr><td><b>EFFECTIVE DATE</b>
xx/xx/xx</td><td><b>REVISED DATE</b>
xx/xx/xx</td></tr>
<tr><td colspan="3"><b>Subject:</b>
<b>IDENTITY PROTECTION (IdP)</b></td></tr>
</table>

1 PURPOSE AND SCOPE

The provisions of this guide are policy for all TRICARE Management Activity (TMA) Components (TMA Directorates; TRICARE Regional Offices (TRO); and the Program Executive Officer (PEO), Joint Medical Information Systems Office (JMISO)). For TRICARE Contractors, this document is policy if required by contract; otherwise it serves as information assurance guidance. The Chief Information Officers of the Service Medical Departments are encouraged to incorporate this document into their information assurance polices and procedures.

1.1 This implementation document provides guidance for accomplishing Department of Defense (DoD) electronic Identity Protection (IdP) activities within the Military Health System (MHS) and supplements the direction provided in DoD Directive (DoDD) 1000.25 (reference a). Federal standardization for credentials is driven by Federal Information Processing Standards Publication (FIPS Pub) 201 (reference b), Personal Identity Verification (PIV) of Federal Employees and Contractors. DoD is also standardizing through DoDD 1000.25 which is compliant with FIPS Pub 201 by using Common Access Card (CAC), Public Key Infrastructure (PKI), and other approved identity management systems.

1.2 DoDD 1000.25 establishes Defense Enrollment Eligibility Reporting System (DEERS) as the authoritative source for identity and verification for DoD. DEERS is a central data repository system. Based on DEERS information, the definitive identity (ID) credential of affiliation with DoD will be issued by Real-Time Automated Personnel Identification System (RAPIDS). Individual information technology (IT) system access control remains a local responsibility.

1.3 DoD Instruction (DoDI) 8520.2 (reference c) implements policy, assigns responsibilities, and prescribes procedures for establishing and using the DoD Public Key Infrastructure (PKI) for authentication, digital signature and encryption in alignment with Information Assurance policy and guidance. DoD PKI provides a common, high assurance level of identification and authentication for the Global Information Grid and is essential to providing enhanced Identity Management capabilities. MHS PKI guidance is contained in MHS Information Assurance (IA) Implementation Guide No.11 (reference d). Joint Task Force – Global Network Operations (JTF-GNO) Communications Tasking Order (CTO)

06-02 (reference e), “Tasks for Phase 1 of Accelerated PKI Implementation,” dated 17 January 2006, mandated use of DoD PKI CAC for network logon and authentication to DoD private Web servers and reporting any non-compliance by summer 2006.

2 IDENTITY PROTECTION CONCEPTS

2.1 Establishment of identity is a basic business function. In the past, identity in the electronic environment was taken for granted: people were who they claimed to be. However, assumptions about identity can create security issues. IdP starts with methods to determine if the person is who he or she says he or she is. The business process of validating the identity includes providing evidence of identity (e.g., checks of public records, background investigations, examination of primary documents, and a face-to-face interaction between the individual and a trusted representative).

2.2 Once the ID is validated, the IdP process continues with a registration process that connects (or “binds”) the identity with other attributes. This electronically stored information is maintained and protected from unauthorized disclosure and use by a security management system. Along with this, an electronic ID credential (e.g., username/password, PKI certificate(s)) is issued to the individual for his/her exclusive use (not to be shared with others).

2.3 The credential is used during the authentication process to establish that the person communicating electronically is who he/she claims to be. The authentication of the user is the first step to gaining access privileges. Authorizing access and granting privileges to a user are separate functions from the authentication step. Access control decisions are made uniquely by each IT system. This guide does not specify methods for authorization or access control decisions.

2.4 Previous to issuance of new IdP guidance individual IT systems developed their own processes for establishing identity and issuing credentials. This created inefficiencies, interoperability difficulties, and IA vulnerabilities because each IT system collected different data; the data was not tied together, so if information was removed from one IT system there was no guarantee that it would also be removed from another; and personal information was stored in many places.

2.5 Users wanting electronic access to DoD information technology (IT) systems or data should be authenticated against DEERS. DEERS is the authoritative source for a person's identity and affiliation with DoD. Utilizing one authoritative source reduces inefficiencies, duplication of data and function, promotes interoperability, minimizes the need for individual privacy information to be stored in multiple locations, enhances IA, and supports the Global Information Grid.

3 GUIDANCE

3.1 MHS IT systems shall follow DoD policy and guidance for IdP (references a, c, and e).

3.2 IT systems shall use ID credentials provided by DoD IdP systems that are approved and authorized under DoDD 1000.25, whenever possible. IT systems shall migrate away from issuing IT system-unique credentials and start using DoD identity credentials and authentication services as the primary means for identifying individuals electronically.

3.3 IT systems shall continue to determine and maintain access controls including role-based access and permissions. IT systems should establish and document their criteria for authorizing access and privileges to individuals.

3.3.1 Access and authentication shall be part of the audit tracking requirements as defined under MHS IA Implementation Guide No.7 (reference f).

3.4 IT systems must authenticate ID credentials with the issuing ID system each time the credentials are used or required to be presented to access an IT system, portal, or application, unless the IT system or application is being accessed from a portal which authenticated the original credential and passed the identity and authentication to the present IT system.

3.5 IT systems shall exchange identity and identity authentication-related information through open security standards as approved by DoD in the Defense Information Technology Standards Registry (DISR) and as interoperable with the Network Centric Enterprise Services (NCES) Security Architecture and federal E-Authentication Architecture.

3.6 If a portal is used for user authentication, it can forward the authentication to the IT system or application as long as there has not been inactivity from the user to the IT system, portal, or application for 15 minutes or longer.

3.7 After 15 minutes of inactivity, the user must be requested to provide the ID credential again, and it must be authenticated with the issuing ID system. (If a user is in an application that has been idle for 15 minutes, proof must be provided that the same user is returning.)

4 RESPONSIBILITIES

4.1 JMISO will:

4.1.1 Include IdP as part of the MHS Service Oriented Architecture Concept.

4.1.2 Establish and execute a strategy to migrate centrally managed IT systems to meet IdP requirements.

4.1.3 Provide direction and oversight to centrally managed programs to ensure that they incorporate and follow IdP guidance.

4.1.4 Validate that IdP requirements are met during Certification and Accreditation of IT systems.

4.1.5 Coordinate with the Services to ensure that centrally managed IT systems are compatible with Service IdP guidance.

4.2 Program Managers of JMISO and TMA IT systems will:

4.2.1 Begin migration planning and implementation of procedures (for centrally managed IT systems) to implement IdP policy. Those plans and procedures should be reflected in their portfolio management plans.

4.2.2 Follow a process to implement DoD Personnel Identity Protection (PIP) and identity authentication requirements for IT systems.

a. Conduct an authentication requirements analysis and risk assessment for IT systems and applications utilizing Office of Management and Budget (OMB) M-04-04 (reference g) and National Institute of Standards and Technology (NIST) SP 800-63 (reference h) which includes mapping identified risks to the applicable assurance level.

b. Select technology based on technical guidance

c. Validate that the implemented application has achieved the required assurance level

d. Periodically reassess the IT system(s) to determine technology refresh requirements and update of PKI server certificates

4.2.3 Use DoD approved Certificate Service Provider (CSP) for identity credentials, and plan for migration to DoD approved CSP identity credentials for users and away from IT systems issuing identity credentials. IT systems will continue to make authorization determinations (access control).

4.2.4 Ensure that user identity is authenticated through a trust relationship approved by DoD.

4.2.5 Ensure that DoD PIP and authentication requirements are included in development contracts and are met by the contractor.

4.2.6 Verify IT system or application compatibility with DoD authentication systems and credentials by conducting interoperability and compatibility testing.

4.2.7 Include identity protection and authentication plans and status in budget justifications (IT Exhibit 300), DoD IT reporting systems (IT Registry), and enterprise architecture planning and documents.

4.2.8 Comply with DoD technical and architectural direction for transmission of identities and identity information among IT systems.

4.3 Service Medical Departments should:

4.3.1 Follow Service guidance regarding IdP and notify JMISO and the MHS Chief Information Officer (CIO) should there be conflicts between this guide and Service guidance.

4.3.2 Ensure that Service personnel follow procedures for IdP when using MHS centrally managed IT systems.

4.4 All Users shall:

4.4.1 Maintain proper affiliation information with the DoD personnel information repository (DEERS) and follow IA procedures regarding their identities and identity credentials.

4.4.2 Protect their identity credentials (e.g., user name and password, PKI certificate/Common Access Card [CAC]).

4.4.3 Use their DoD issued identity credentials for DoD business only.

4.4.4 Protect their personal information (e.g., Social Security Number [SSN]) from disclosure.

5 REFERENCES

a. DoD Directive 1000.25, "Personnel Identity Protection (PIP) Program," 19 July 2004

b. FIPS Pub 201, Federal Information Processing Standards Publication (FIPS Pub) 201, "Personal Identity Verification (PIV) of Federal Employees and Contractors," 25 February 2005

c. DoD Instruction 8520.2, "Public Key Infrastructure (PKI) and Public Key Enabling (PKE)," 1 April 2004

d. MHS IA Implementation Guide No.11, "DoD Public Key Infrastructure (PKI) and Public Key Enabling (PKE)"

e. Joint Task Force – Global Network Operations Communications Tasking Order (JTF-GNO CTO) 06-02, "Tasks for Phase 1 of Accelerated PKI Implementation," 17 January 2006

f. MHS IA Implementation Guide No.7, "Data Integrity"

g. Office of Management and Budget (OMB), Executive Office of the President Memo, "Implementation of the Government Paperwork Elimination Act," M-04-04, E-Authentication Guidance for Federal Agencies, 16 December 2003

h. National Institute of Standards and Technology (NIST), "Electronic Authentication Guideline," September 2004, Special Publication 800-63, (SP 800-63)

i. DoD Directive 5230.9, "Clearance of DoD Information for Public Release," 9 April 1996

j. DoD Instruction 5230.29, "Security and Policy Review of DoD Information for Public Release," 6 August 1999

6 ACRONYMS

CAC	Common Access Card
CIO	Chief Information Officer
CSP	Certificate Service Provider
CTO	Communications Tasking Order
DEERS	Defense Enrollment Eligibility Reporting System
DISR	Defense Information Technology Standards Registry
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
IA	Information Assurance
ID	Identity
IdP	Identity Protection
IT	Information Technology
JMISO	Joint Medical Information Systems Office

JTF-GNO	Joint Task Force-Global Network Operations
MHS	Military Health System
NCES	Network Centric Enterprise Services
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PEO	Program Executive Officer
PIN	Personal Identification Number
PIP	Personnel Identity Protection
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
RAPIDS	Real-Time Automated Personnel Identification System
SSN	Social Security Number
TMA	TRICARE Management Activity
TRO	TRICARE Regional Office

7 DEFINITIONS

Authentication – Establishing, with a high degree of confidence, that the identity presented by the individual is that of the individual. Usually involves an individual making a claim regarding their identity (e.g., providing an identifier, username, CAC) and then providing a personal qualifier that validates that the claim is true (e.g., password, Personnel Identification Number (PIN)).

Authorization – The process of ensuring that individuals have a need to access and currently meet all the criteria before being granted access.

DoD Private Web Server – For unclassified networks, a DoD private Web server is any DoD-owned, operated, or controlled Web server providing access to sensitive information that has not been reviewed and approved for release in accordance with DoDD 5230.9 (reference h) and DoDI 5230.29 (reference i).

Identity Credential – A token (Username/Password, PIN, PKI certificate, etc.) which is bound to the individual's physical identity through the processes of a trusted credentialing source which can substantiate its authenticity when presented to an IT system or network by the individual as proof of his/her identity.

Personnel Identity Protection (PIP) Program – A business process that authenticates identity and involves:

a. Binding individual ID to an ID protection system through issuance of a credential

b. Linkage of credential to individual through characteristics and ID number

c. Digital authentication of credential linkage to the individual

Military Health System Information Assurance Implementation Guide Number 15 for Identity Protection

COORDINATION

CoS, TMA	Col Charles Wolak	Concur 7/06/06
Deputy Director, TMA	MG Elder Granger	Concur 7/10/06
DoD OGC	Mr. John Casciotti	____________________
DASD, FHP&R	Ms. Ellen Embrey	Concur 8/23/06
CoS (HA)	COL Thom Kurmel	____________________
PDASD (HA)	Dr. Steve Jones	____________________